**南阳市公共资源交易中心**

**日志分析报告**

**（2017年3月28日）**



河南凌云交汇软件有限公司

JOINSOFT®

河南省南阳市两相东路创业大厦1801室473000

电话：+0377-62375119

传真：+0377-62375119

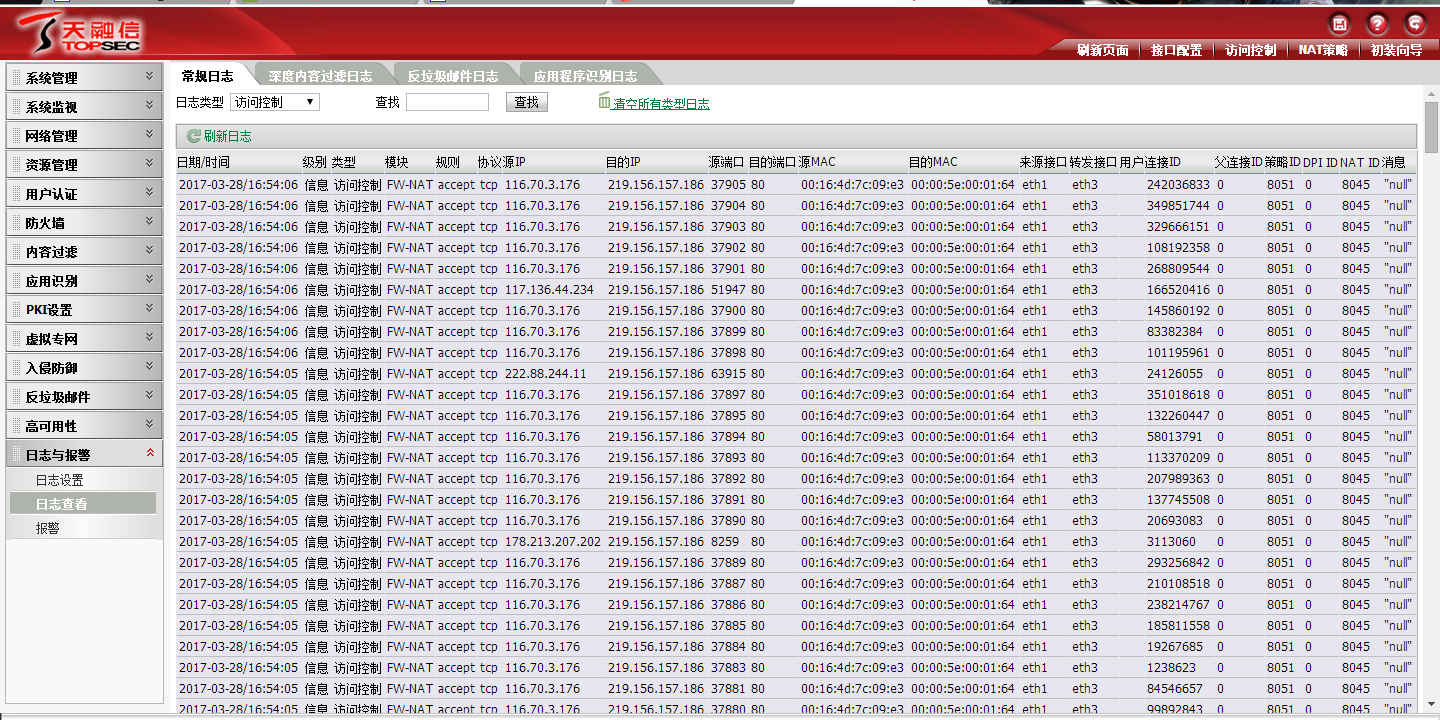
http://lyjhsoft.com.cn

2017年3月28日对安全设备进行了日志分析与安全审计，安全设备包括防火墙、入侵防御、WEB防火墙1、WEB防火墙2、安全管理平台、核心交换机。安全审计内容包括：系统信息、设备版本及基本配置、接口配置与状态、日志信息状态、访问控制；主要审计访问控制。对相关内容进行截图。

# 日志分析

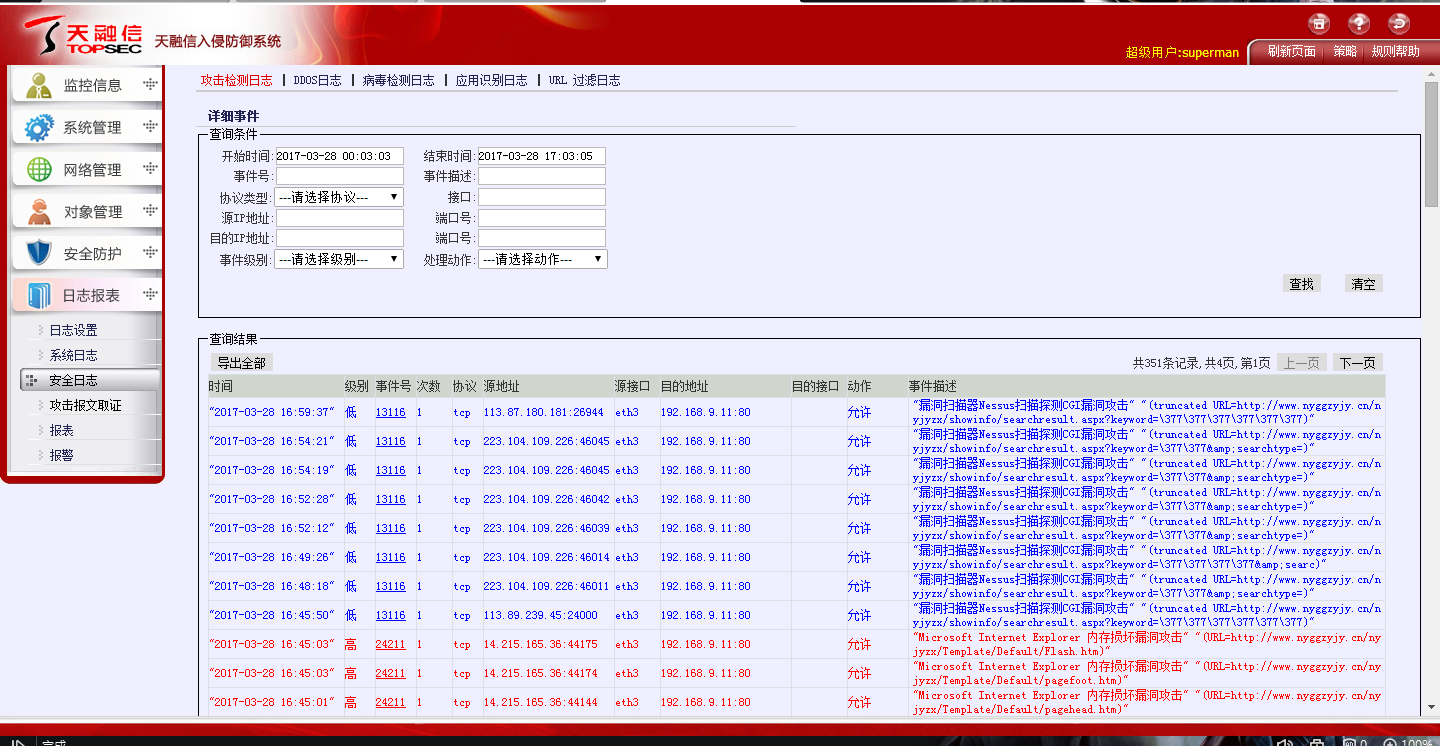
## 防火墙日志

防火墙开启访问控制日志，访问控制记录了事件日期/时间、级别、协议源IP、目的IP、目的端口等信息。



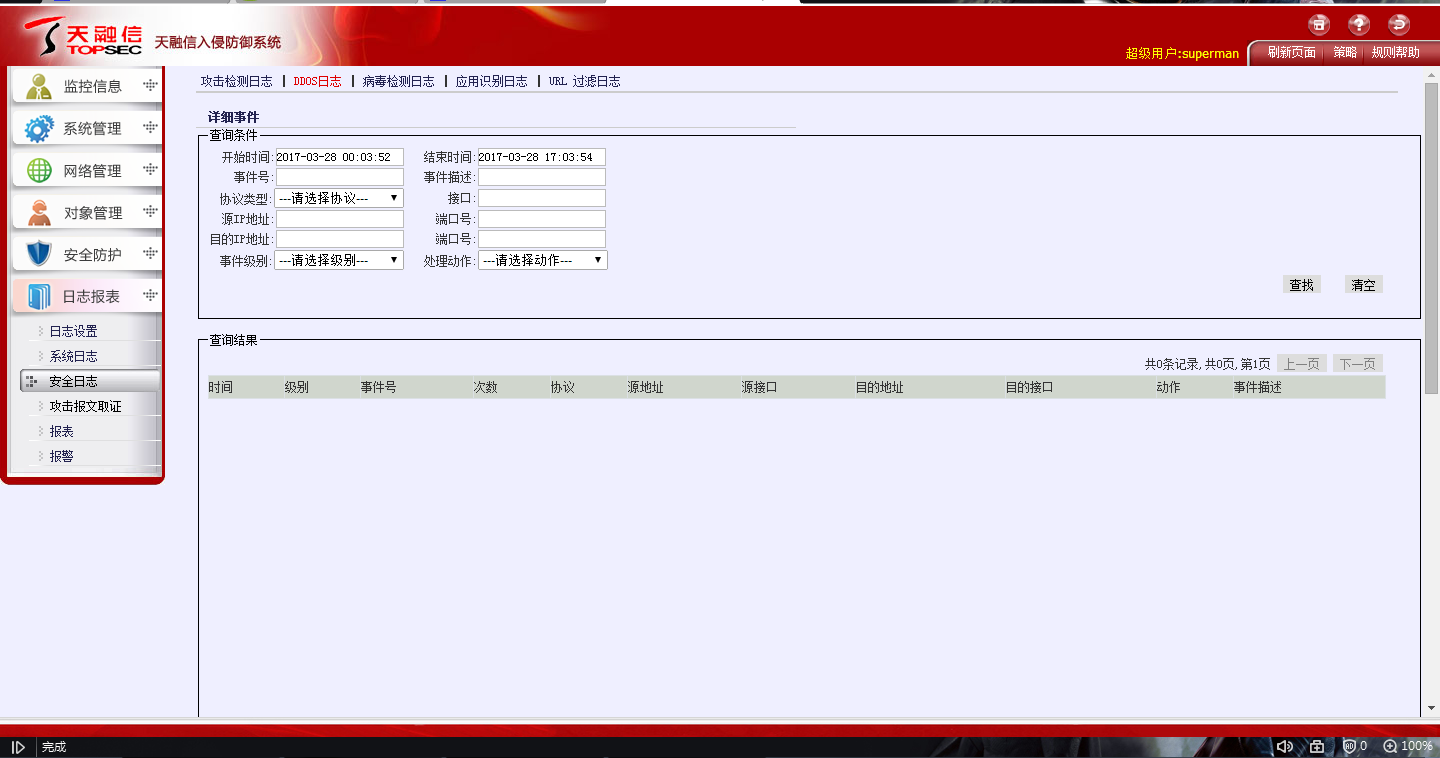
## 入侵防御日志

1. 入侵防御开启攻击检测日志，2017年3月28日零点到16：55分，共记录351条，其中事件级别为高的共36条记录。



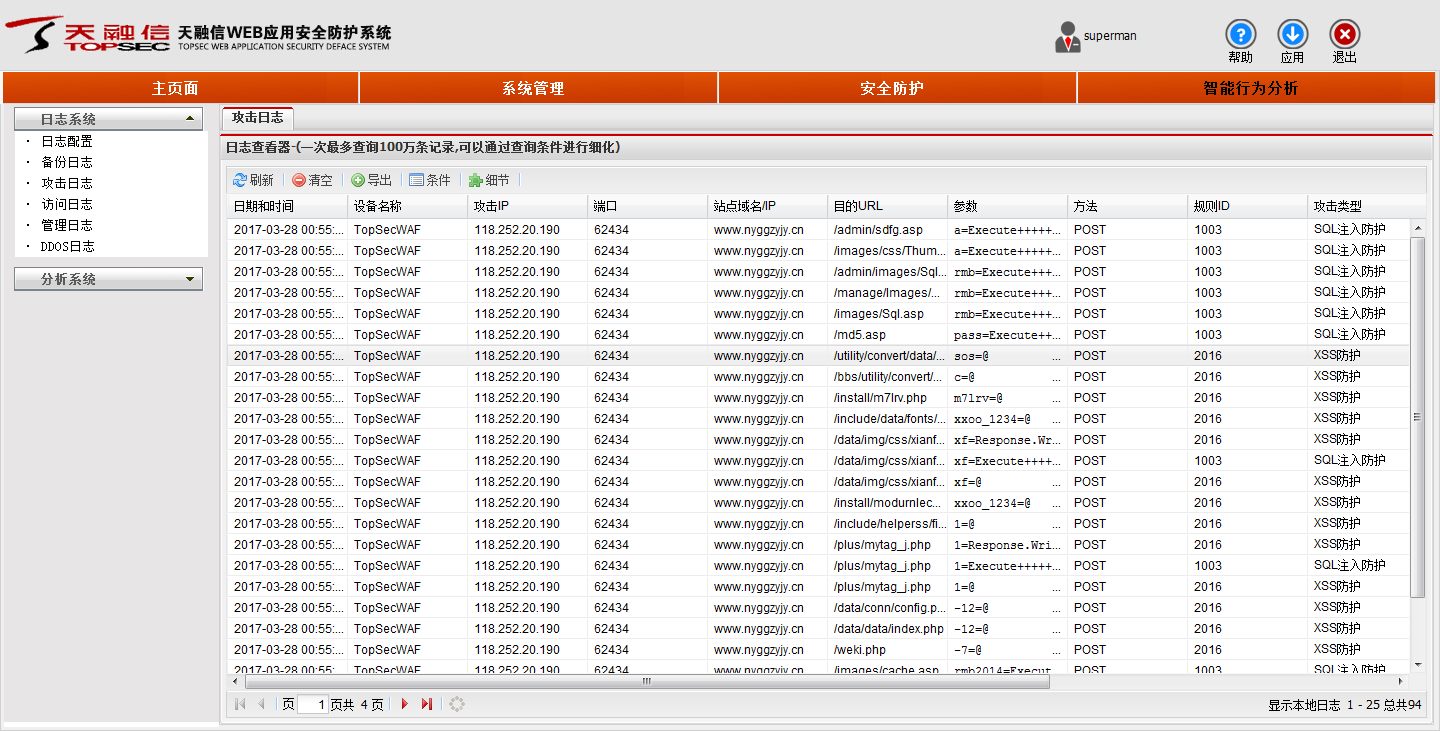
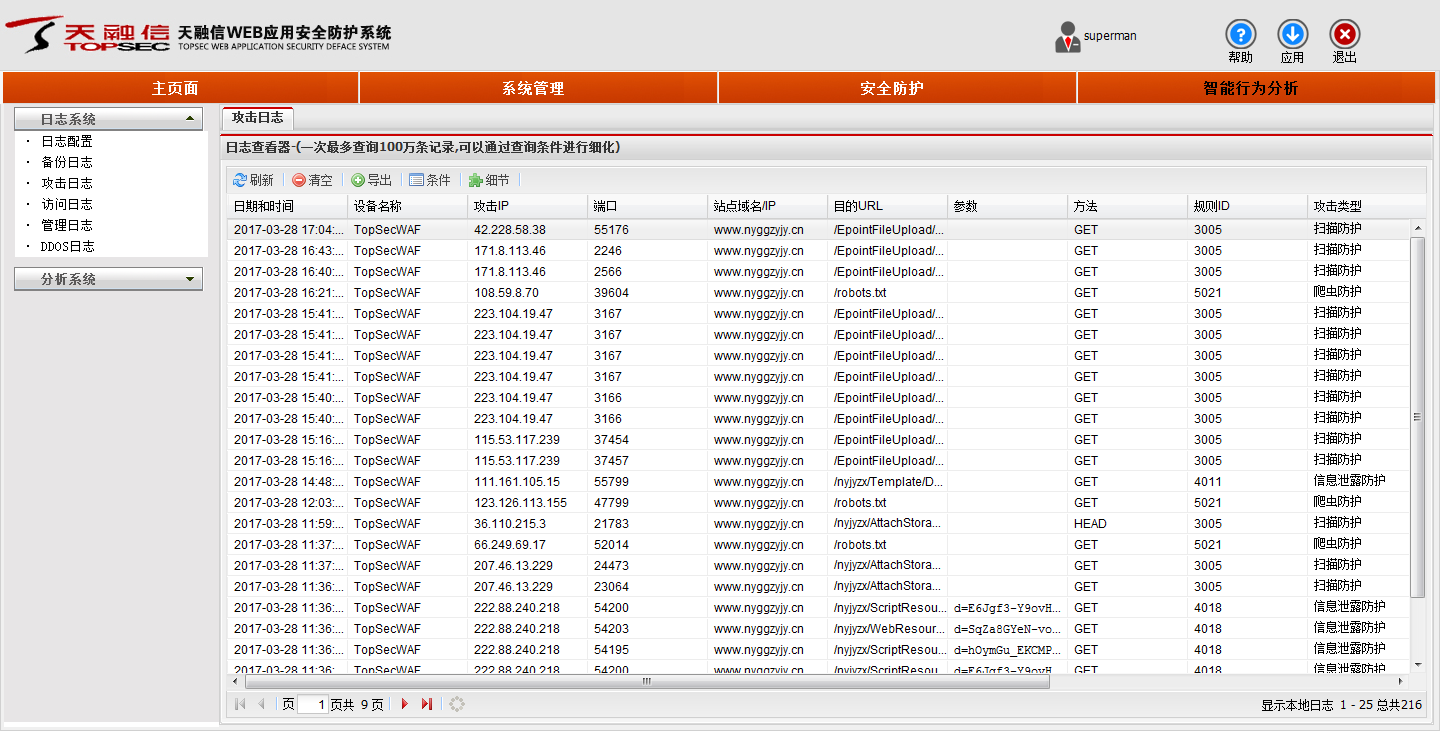


1. 入侵防御开启攻击DDOS日志，2017年3月28日共查询到0条攻击记录，事件级别为高.

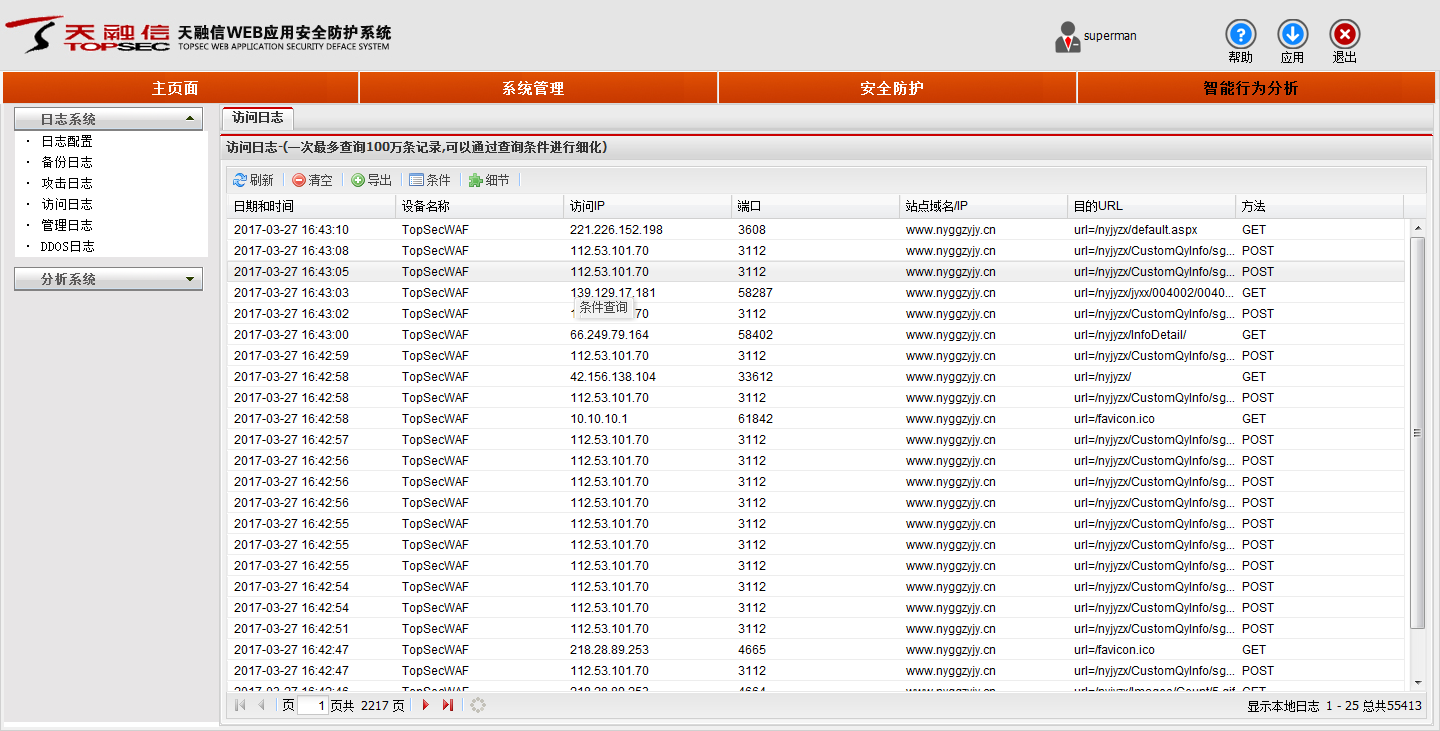


## WEB防火墙1（192.168.9.2）

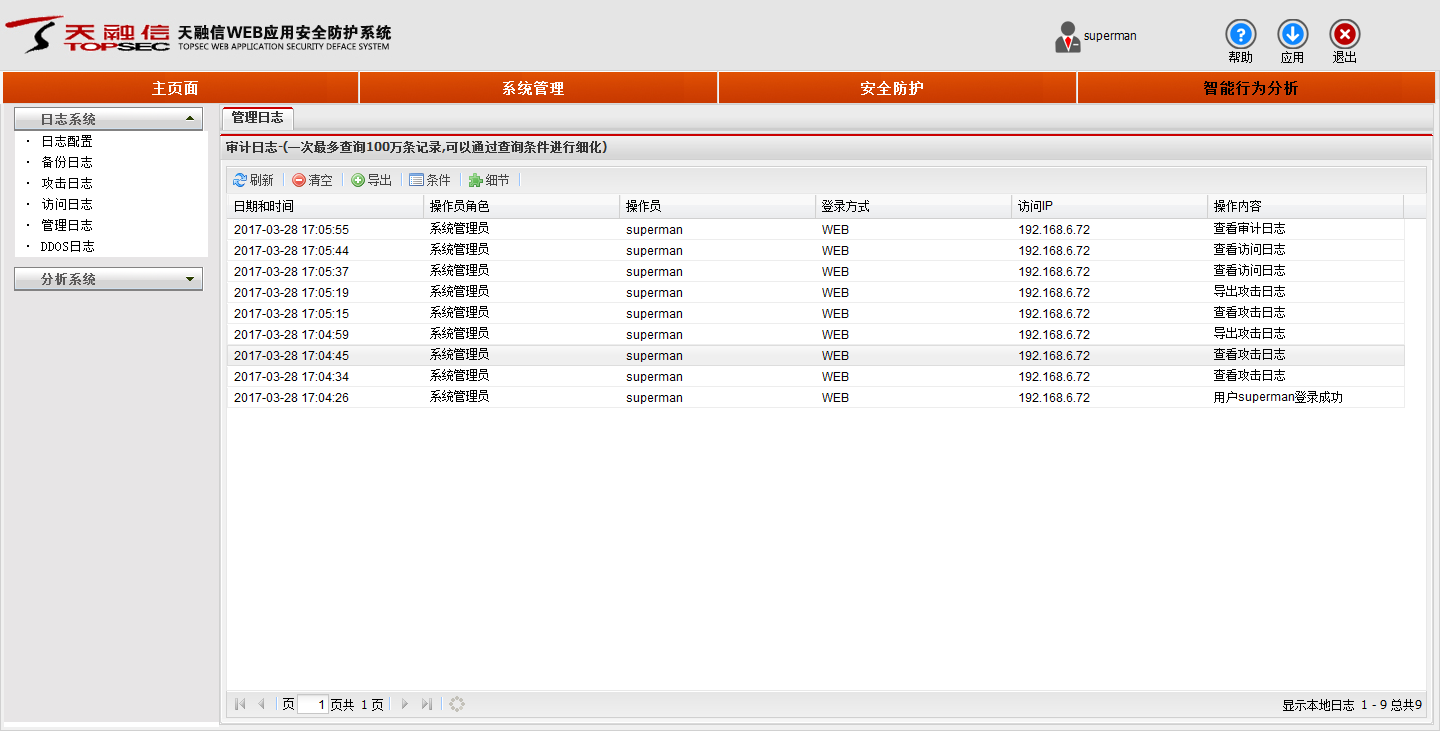
1. WEB防火墙攻击日志开启，经查询2017年3月28日共找记录216条，经过筛选严重级别的94条。



1. WEB防火墙访问日志开启，经查询2017年3月28日共找记录46573条.



1. WEB防火墙管理日志开启，经查询2017年3月28日共找记录9条。

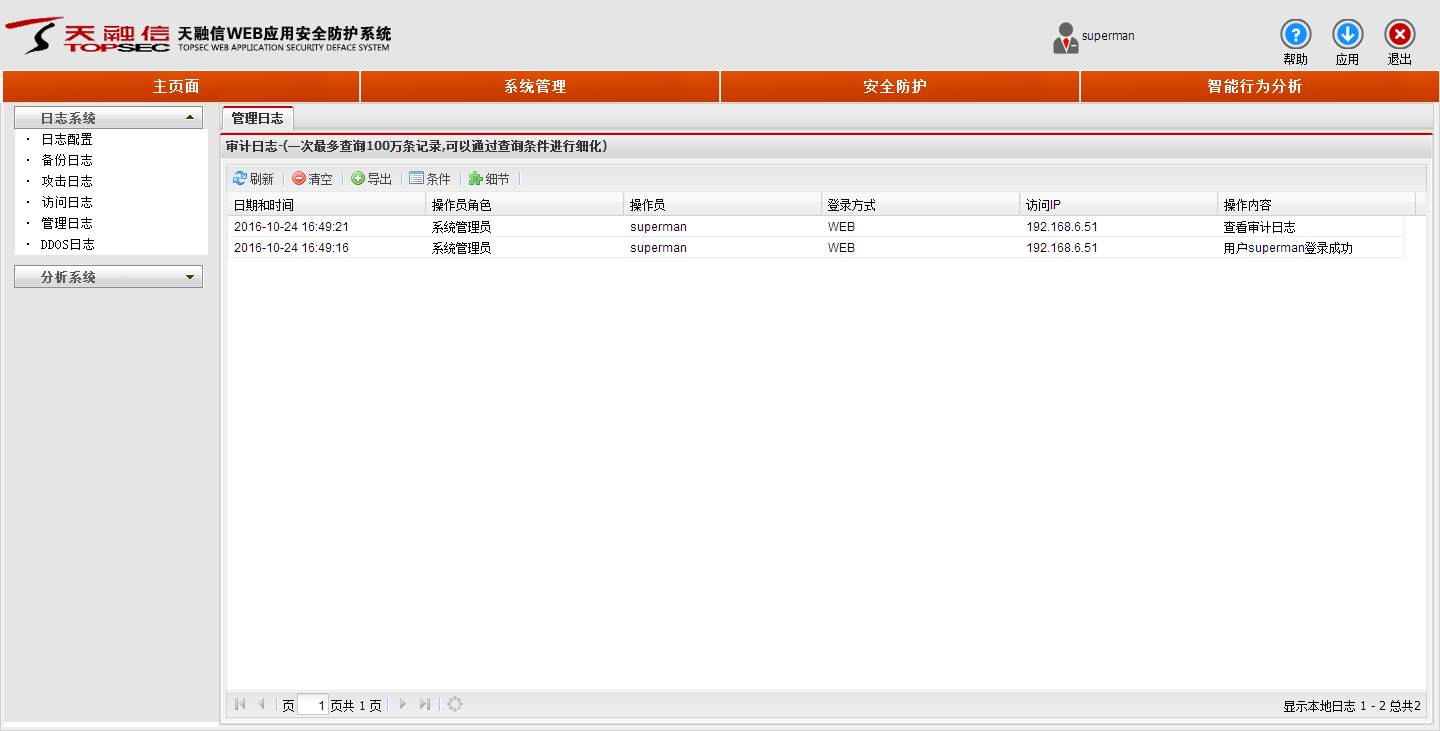


## WEB防火墙2（192.168.9.3）

1、WEB防火墙攻击日志开启，经查询2017年3月28日共找记录0条。

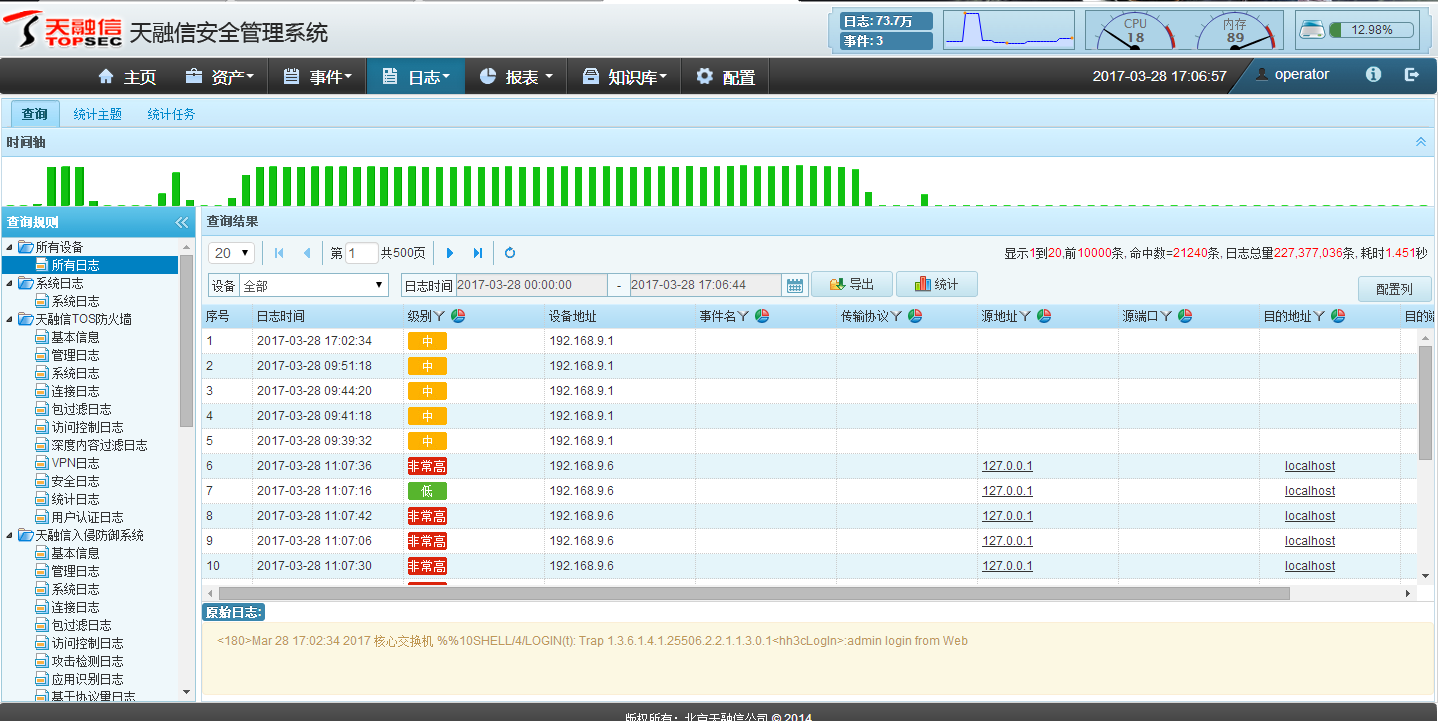


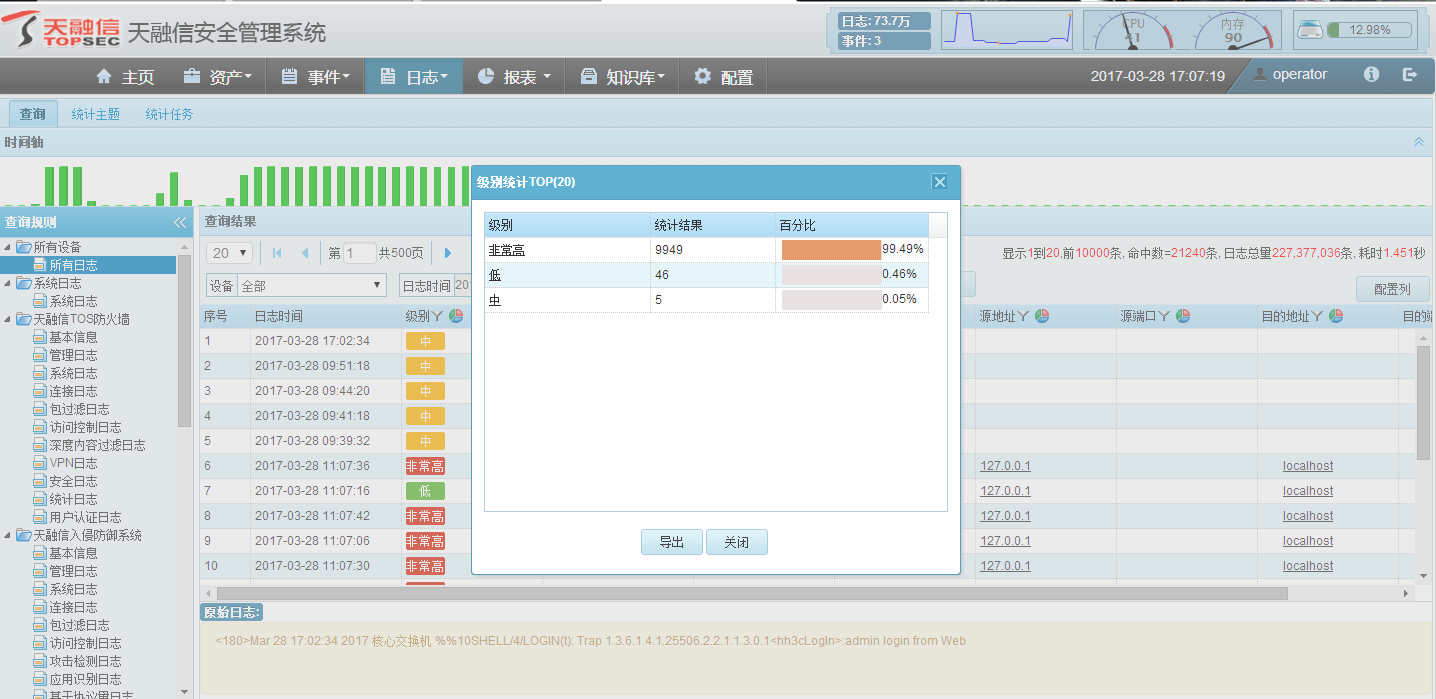
2、WEB防火墙管理日志开启，经查询2017年3月28日共找记录2条。



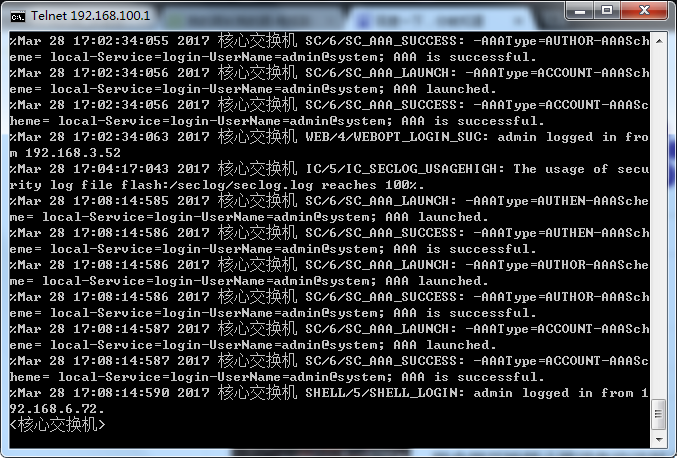
## 安全管理平台

1. 安全管理平台日志开启，经查询2017年3月28日共找记录227377036条。





## 核心交换机



# 问题与解决办法

此次对安全设备的日志分析进行了分析，主要对防火墙的访问日志进行了查询，入侵防御主要开启了攻击日志检测与DDOS检测，对WEB防火墙的攻击日志、访问日志、管理日志进行了查询，发现访问控制记录了事件日期/时间、级别等相关信息；入侵防御记录的攻击日志主要是SQL注入攻击和CGI漏洞攻击；WEB防火墙攻击日志中主要记录的是SQL注入攻击以及扫描防护，同时对安全设备的账户权限进行了检查。

SQL注入攻击，就是攻击者通过欺骗数据库服务器执行非授权的任意查询过程。攻击者通过SQL注入可获取管理员权限，进而操作后台数据，篡改网页内容。

CGI漏洞攻击是通过CGI漏洞执行远程命令执行的操作过程，攻击者通过该漏洞可直接获取系统敏感数据以及权限提升。

从分析中可以看出，WAF有效的检测并阻断各类攻击，避免SQL注入漏洞以及CGI漏洞的检测和攻击，解决了SQL注入带来的危害，通过报表统计可以看到攻击的来源，能够更有效的追溯攻击来源，使得网站的安全得到保障。

信息泄露攻击手段是通过扫描器对web应用进行扫描，访问敏感文件获取信息泄露的攻击方法。

内存损坏攻击是Internet Explorer 7-11版本，没有正确访问内存对象，在实现上存在远程代码执行漏洞，攻击者利用此漏洞可在当前用户上下文中执行任意代码。

从分析中可以看出，WAF有效的检测并阻断各类攻击，避免SQL注入漏洞以及信息泄露的检测和攻击，解决了SQL注入带来的危害，通过报表统计可以看到攻击的来源，能够更有效的追溯攻击来源，使得网站的安全得到保障。

交易中心信息科确认人： 提交人：

日期： 日期：